

(19)日本国特許庁(J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号

特開2002-358283

(P2002-358283A)

(43)公開日 平成14年12月13日(2002. 12. 13)

(51)Int.Cl. ⁷	識別記号	F I	テ-マ-ト*(参考)
G 0 6 F 15/00	3 3 0	G 0 6 F 15/00	3 3 0 B 5 B 0 8 5
H 0 4 L 9/32		H 0 4 L 9/00	6 7 5 D 5 J 1 0 4

審査請求 有 請求項の数26 O L (全 16 頁)

(21)出願番号 特願2001-166114(P2001-166114)

(22)出願日 平成13年6月1日(2001. 6. 1)

(71)出願人 000004237

日本電気株式会社

東京都港区芝五丁目7番1号

(72)発明者 田中 広幸

東京都港区芝五丁目7番1号 日本電気株式会社内

(74)代理人 100080816

弁理士 加藤 朝道

Fターム(参考) 5B085 AC12 AE02 AE23 BG07

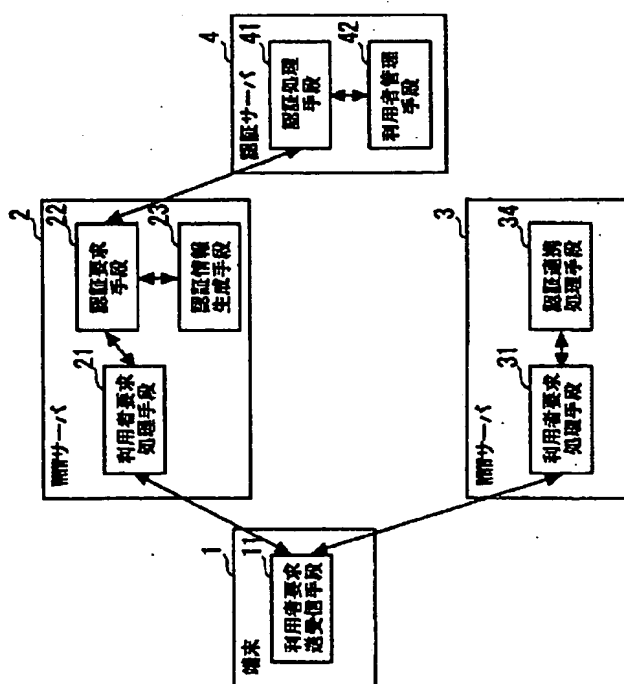
5J104 AA07 MA04 PA07

(54)【発明の名称】 利用者認証連携方法及びシステム及びプログラム

(57)【要約】

【課題】認証を行うサーバを利用できないWWWサーバでも、認証の連携を可能とする利用者認証連携システム及び方法の提供。

【解決手段】WWWサーバ2は、端末1が、利用者からの要求と、利用者認証を行うための利用者情報を受信し、前記利用者情報を認証サーバ4に送信する手段21、22と、認証サーバ4での認証が成功した場合に、前記利用者の前記利用者情報と時間情報から認証情報の生成する認証情報生成手段23と、前記生成された認証情報を、要求結果と共に、前記端末に送信する手段21と、を備え、端末1は、WWWサーバ3に要求を送信する場合、認証情報を送信し、WWWサーバ3は認証情報から、利用者情報と時間情報を取り出し、認証の連携処理を行う認証連携処理手段34と、認証情報の正しさが検証され、前記利用者が認証された場合は、前記利用者の要求を受け付け、要求結果と共に、新たに生成した認証情報を、前記端末に送信する手段31とを備える。



【特許請求の範囲】

【請求項1】端末からネットワークを介してアクセスされる一の情報提供サーバが、前記端末から送信された利用者情報を受け取り、前記利用者情報と時間情報とから認証情報を生成するステップと、

前記一の情報提供サーバが、生成した前記認証情報を、前記端末に送信するステップと、

前記端末からネットワークを介してアクセスされる情報提供サーバであって、認証の連携処理を行う情報提供サーバが、前記端末から送信された前記認証情報を受け取り、前記認証情報から、利用者情報と時間情報を取り出して、認証判定を行うステップと、

を含む、ことを特徴とする利用者認証連携方法。

【請求項2】前記一の情報提供サーバは、前記端末から前記一の情報提供サーバに送信された前記利用者情報を、前記一の情報提供サーバに接続する認証サーバに送信するステップを実行し、前記認証サーバで認証が正しく行われた場合に、前記認証サーバでの認証結果を受けた前記一の情報提供サーバにおいて、前記認証情報を生成するステップと、前記認証情報を前記端末に送信するステップと、が実行される、ことを特徴とする請求項1記載の利用者認証連携方法。

【請求項3】前記認証判定を行うステップで、認証が成功した場合、認証の連携処理を行う前記情報提供サーバでは、前記認証情報から前記利用者情報を取り出し、前記利用者情報と時間情報とから、あらたに認証情報を生成し、前記端末に、あらたに生成された前記認証情報を送信するステップを含む、ことを特徴とする請求項1記載の利用者認証連携方法。

【請求項4】あらたに生成された前記認証情報を受信した前記端末が、認証の連携処理を行う情報提供サーバに要求を送信する場合に、前記認証情報を、認証の連携処理を行う前記情報提供サーバに送信するステップと、認証の連携処理を行う前記情報提供サーバでは、前記端末から送信された前記認証情報を受け取り、前記認証情報から利用者情報と時間情報を取り出して、認証判定を行い、認証が成功した場合、前記認証情報から取り出された前記利用者情報と、時間情報から、あらたに認証情報を生成し、前記端末に、あらたに生成された前記認証情報を送信するステップと、を含む、ことを特徴とする請求項3記載の利用者認証連携方法。

【請求項5】前記認証情報の生成に用いられる前記時間情報が、前記認証情報を生成する情報提供サーバのシステム時計の時間情報である、ことを特徴とする請求項1乃至4のいずれかに記載の利用者認証連携方法。

【請求項6】端末が、利用者からの要求と、利用者認証を行うための利用者情報を、一の情報提供サーバに送信するステップと、

前記一の情報提供サーバでは、前記利用者情報を、前記

一の情報提供サーバが接続する認証サーバに送信し、前記認証サーバでの認証が成功した場合に、前記一の情報提供サーバの認証情報生成部にて、認証情報を生成するステップと、

前記一の情報提供サーバは、前記一の情報提供サーバの前記認証情報生成部で生成された前記認証情報を、要求結果と共に、前記端末に送信するステップと、

前記端末が、前記一の情報提供サーバと連携し、認証の連携処理を行う他の情報提供サーバに要求を送信する場合、前記要求とともに、前記認証情報を、前記他の情報提供サーバを送信するステップと、

前記他の情報提供サーバでは、前記端末から送信された前記認証情報を受け取り、認証連携処理部で、受け取った前記認証情報を基に、認証の連携処理を行うステップと、

前記他の情報提供サーバにおいて、前記認証の連携処理によって、認証情報の正しさが検証され、前記利用者が認証された場合には、前記利用者の要求を受け付け、要求結果と共に、新たに生成した認証情報を、前記端末に送信するステップと、

を有する、ことを特徴とする利用者認証連携方法。

【請求項7】前記認証情報生成部で生成される認証情報が、利用者情報と時間情報と、チェックデータとを含み、これらの情報が暗号化されている、ことを特徴とする請求項6記載の利用者認証連携方法。

【請求項8】前記認証連携処理部で認証の連携処理を行うステップが、

受け取った前記認証情報を復号するステップと、

復号された前記認証情報のチェックデータを検査するステップと、

前記チェックデータの検査が成功した場合、復号された前記認証情報から利用者情報と時間情報を取り出すステップと、

前記取り出された時間情報に基づき時間の検査を行うステップと、

前記時間検査が成功した場合、認証成功とするステップと、

を含む、ことを特徴とする請求項6又は7記載の利用者認証連携方法。

【請求項9】利用者からの要求に対し、最初の情報提供サーバへのアクセスの場合、前記認証サーバを利用した利用者認証処理を行い、

続く情報提供サーバへのアクセスでは情報提供サーバでの認証連携処理を行う、ことを特徴とする請求項6又は7記載の利用者認証連携方法。

【請求項10】前記一の情報提供サーバが認証の認証連携を行う認証連携処理部を有し、

前記一の情報提供サーバでは、前記端末から送信された認証情報を受け取り、前記認証連携処理部で認証の連携処理を行い、認証判定が成功した場合、前記一の情報提

供サーバの認証情報生成部に認証情報の生成を依頼するステップと、
前記一の情報提供サーバの前記認証情報生成部は、前記一の情報提供サーバの前記認証連携処理部が前記認証情報から取得した利用者情報を受け取り、前記利用者情報と時間情報とから認証情報を生成するステップと、
を含む、ことを特徴とする請求項6記載の利用者認証連携方法。

【請求項11】認証の連携処理を行う前記他の情報提供サーバが認証情報生成部を有し、
前記他の情報提供サーバの認証連携処理部で認証の連携処理を行い、認証判定が成功した場合、前記他の情報提供サーバの認証情報生成部に認証情報の生成を依頼するステップと、
前記他の情報提供サーバの認証情報生成部は、前記認証連携処理部が前記認証情報から取得した利用者情報を受け取り、前記利用者情報と時間情報とから認証情報を生成するステップと、
前記他の情報提供サーバが、利用者の要求結果と、生成した前記認証情報を前記端末に送信するステップと、
を含む、ことを特徴とする請求項6又は10記載の利用者認証連携方法。

【請求項12】端末からネットワークを介してアクセスされる一の情報提供サーバが、
前記端末から入力され前記一の情報提供サーバに送信された利用者情報と、前記一の情報提供サーバでの時間情報とから認証情報を生成し、生成した前記認証情報を、前記端末に送信する手段を備え、
前記端末からネットワークを介してアクセスされる情報提供サーバであって、認証の連携処理を行う情報提供サーバが、前記端末から送信された前記認証情報を受け取り、前記認証情報を復号して利用者情報及び時間情報を取り出し、認証判定を行う手段を備えている、ことを特徴とする利用者認証連携システム。

【請求項13】端末と、該端末からネットワークを介してアクセスされる複数の情報提供サーバと、を有し、
前記複数の情報提供サーバには、認証サーバに接続される少なくとも一つの情報提供サーバと、認証の連携処理を行う少なくとも一つの情報提供サーバと、が含まれ、
前記認証サーバに接続される一の情報提供サーバは、前記端末が、利用者からの要求と、利用者認証を行うための利用者情報を、前記一の情報提供サーバに送信した場合、これを受信し、前記利用者情報を、前記認証サーバに送信する手段と、
前記認証サーバでの認証が成功した場合に、前記利用者情報と時間情報から認証情報を生成する認証情報生成手段と、
前記生成された認証情報を、要求結果と共に、前記端末に送信する手段と、
を備え、

前記端末は、認証の連携処理を行う前記情報提供サーバに要求を送信する場合、前記一の情報提供サーバより送信された前記認証情報を、認証の連携処理を行う前記情報提供サーバに送信する手段を備え、

認証の連携処理を行う前記情報提供サーバは、前記認証情報から、利用者情報と時間情報を取り出し、認証の連携処理を行う認証連携処理手段と、
前記認証の連携処理によって、認証情報の正しさが検証され、前記利用者が認証された場合は、前記利用者の要求を受け付け、要求結果と共に、新たに生成した認証情報を、前記端末に送信する手段とを備えている、ことを特徴とする利用者認証連携システム。

【請求項14】前記一の情報提供サーバの前記認証情報生成手段が、前記利用者情報と、時間情報と、チェックデータとからなる情報を暗号化したものを、前記認証情報として出力する、ことを特徴とする請求項13記載の利用者認証連携システム。

【請求項15】利用者からの要求に対し、最初の情報提供サーバへのアクセスの場合、前記認証サーバを利用した利用者認証処理を行い、続くアクセスでは、情報提供サーバの認証連携処理を行うことを特徴とする請求項13記載の利用者認証連携システム。

【請求項16】前記一の情報提供サーバが、
前記端末からの利用者の要求を処理する利用者要求処理手段と、
前記認証サーバに対して認証要求を行い、前記認証サーバで認証が成功した場合、認証情報を生成するように要求する認証要求手段と、
を備え、

前記認証情報生成手段は、前記認証要求手段からの要求を受けて、前記利用者情報と時間情報とから前記認証情報を生成し、
前記利用者要求処理手段は、前記端末に対して、要求結果と、前記生成された認証情報とを送信する、ことを特徴とする請求項13記載の利用者認証連携システム。

【請求項17】認証の連携処理を行う前記情報提供サーバが、
前記端末からの利用者の要求を処理する利用者要求処理手段を備え、

前記認証連携処理手段が、前記端末から要求とともに送信される認証情報を受け取り、前記認証情報を基に、認証の連携処理を行い、
前記認証連携処理手段での認証連携処理によって、認証情報の正しさが検証され、前記利用者が認証された場合には、前記利用者要求処理手段では、前記利用者の要求を受け付け、要求結果と共に、新たに生成された前記認証情報を、前記端末に送信する、ことを特徴とする請求項13記載の利用者認証連携システム。

【請求項18】前記認証連携処理手段が、
前記認証情報を復号する手段と、

復号された前記認証情報のチェックデータを検査する手段と、

前記チェックデータの検査結果が正しい場合、復号された前記認証情報から利用者情報と時間情報を取り出す手段と、

前記時間情報の検査を行う手段と、

を含み、前記時間情報の検査結果が正しい場合、認証成功とする、ことを特徴とする請求項 1 3 記載の利用者認証連携システム。

【請求項 1 9】前記一の情報提供サーバが、認証連携処理手段をさらに備え、

前記一の情報提供サーバは、前記端末から送信された認証情報を受け取り、前記一の情報提供サーバの前記認証連携処理手段で認証連携を行い、認証判定が成功した場合、前記一の情報提供サーバの前記認証情報生成手段に対して認証情報の生成を依頼し、

前記一の情報提供サーバの前記認証情報生成手段は、前記認証連携処理手段が前記認証情報から取得した利用者情報を受け取り、前記利用者情報と時間情報から認証情報を生成する、ことを特徴とする請求項 1 3 記載の利用者認証連携システム。

【請求項 2 0】認証の連携処理を行う前記情報提供サーバが、認証情報生成手段を備え、

認証の連携処理を行う前記情報提供サーバが、前記認証連携処理手段で認証連携を行い、認証判定が成功した場合、認証の連携処理を行う前記情報提供サーバの前記認証情報生成手段に認証情報の生成を依頼し、

認証の連携処理を行う前記情報提供サーバの前記認証情報生成手段が、前記認証連携処理手段が前記認証情報から取得した利用者情報を受け取り、利用者情報と時間情報とから認証情報を生成し、利用者の要求結果と前記認証情報を前記端末に送信する、ことを特徴とする請求項 1 3 又は 1 9 記載の利用者認証連携システム。

【請求項 2 1】端末からネットワークを介してアクセスされる一の情報提供サーバが、

(a) 前記端末から利用者からの要求と、利用者認証を行うための利用者情報を受信し、前記利用者情報を、前記認証サーバに送信する処理と、

(b) 前記認証サーバでの認証が成功した場合に、前記利用者情報と時間情報から認証情報を生成する認証情報生成処理と、

(c) 前記生成された認証情報を、要求結果と共に、前記端末に送信する処理と、

を有し、

端末からネットワークを介してアクセスされ前記一の情報提供サーバと認証の連携処理を行う情報提供サーバが、

(d) 前記端末から送信された前記認証情報から、利用者情報と時間情報を取り出し、認証の連携処理を行う認証連携処理と、

(e) 前記認証連携処理によって、認証情報の正しさが検証され、前記利用者が認証された場合は、前記利用者の要求を受け付け、要求結果と共に、新たに生成した認証情報を、前記端末に送信する処理とを含み、前記各処理を前記各情報提供サーバで実行させるためのプログラム。

【請求項 2 2】請求項 2 1 記載のプログラムにおいて、前記認証情報生成処理で、前記利用者情報と時間情報とチェックデータとから、認証情報を生成し、さらにこの認証情報を暗号化する処理を、

前記情報提供サーバで実行させるためのプログラム。

【請求項 2 3】請求項 2 1 記載のプログラムにおいて、前記認証連携処理が、

前記認証情報を復号する処理と、

復号された前記認証情報のチェックデータを検査する処理と、

前記チェックデータの検査結果が正しい場合、復号された前記認証情報から利用者情報と時間情報を取り出す処理と、

20 前記時間情報の検査を行う処理と、

を含み、

前記各処理を、前記情報提供サーバで実行させるためのプログラム。

【請求項 2 4】端末からネットワークを介してアクセスされる情報提供サーバが、

前記端末より送信される、利用者認証を行うための利用者情報を受信し、前記利用者情報を、前記認証サーバに送信する手段と、

30 前記認証サーバでの認証が成功した場合に、前記利用者情報と時間情報から認証情報を生成する認証情報生成手段と、

前記生成された認証情報を前記端末に送信する手段と、

を備えている、ことを特徴とする情報提供サーバ装置。

【請求項 2 5】端末とネットワーク接続され前記端末より送信される利用者情報を受信し、前記利用者情報と時間情報から認証情報を生成し、前記生成した認証情報を前記端末に送信する手段を備えた情報提供サーバ装置と、

認証の連携処理を行う情報提供サーバであって、

40 前記端末から送信された前記認証情報から、利用者情報と時間情報を取り出し、認証の連携処理を行う認証連携処理手段と、

前記認証の連携処理によって、認証情報の正しさが検証され、前記利用者が認証された場合は、前記利用者の要求を受け付け、要求結果と共に、新たに生成した認証情報を、前記端末に送信する手段とを備えている、ことを特徴とする情報提供サーバ装置。

【請求項 2 6】前記認証連携処理手段が、

前記認証情報を復号する手段と、

復号された前記認証情報のチェックデータを検査する手段と、

前記チェックデータの検査結果が正しい場合、復号された前記認証情報から利用者情報と時間情報を取り出す手段と、
前記時間情報の検査を行う手段と、
を含み、前記時間情報の検査結果が正しい場合、認証成功とする、ことを特徴とする請求項24記載の情報提供サーバ装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、認証システム及び方法に関し、特にサーバで認証連携処理を行う方法とシステムと装置並びにプログラムに関する。

【0002】

【従来の技術】利用者認証連携システムとして、例えば特開平11-31129号公報には、複数のWWW (World Wide Web) サーバを備えたネットワークシステムにおいて、利用者は一度認証すれば、認証有効時間内は、付与された一意の不可視のIDをもとに、複数ページや異なるWWWサーバにわたってアクセスを可能としたWWWサーバ連携システムが提案されている。このWWWサーバ連携システムにおいて、セッションIDを用いて連携を処理するホストは、複数のいずれかのWWWサーバから通知されたブラウザからHTML (HyperText Markup Language) 文書を解析し、セッションIDが付与されていなかったときに、ユーザ情報の入力要求を、WWWサーバを介してブラウザに送信し、送信されたユーザ情報を解析して登録の許可された要求に対して一意のセッションIDを生成し、再び、WWWサーバを介してセッションIDを埋め込んだHTML文書をブラウザに送信するとともに、有効時間情報を管理し、有効時間情報範囲内のとき、認証を許可する。すなわち、認証が必要な場合、端末によって送信されたID、パスワードはWWWサーバを経由してホストに送信され、認証が行われる。ホストによって認証が成功した場合、ホストによりセッションIDが生成され、そのセッションIDは、結果と共にWWWサーバ経由で端末に送られ、利用者からのアクセス時には、端末から送信される要求には、セッションIDが自動的に付加されており、そのセッションIDはホストによって検証される。

【0003】しかしながら、この利用者認証連携システムは、次のような問題点を有している。

【0004】第1の問題点は、ホストが利用できないWWWサーバとは連携ができない、ということである。その理由は、セッションIDの検証、生成が、専ら、ホストで行われる、ためである。

【0005】第2の問題点は、利用者からの要求が増大した場合、そのレスポンスが低下する、ということである。その理由は、すべてのWWWサーバは、すべての利用者からのアクセスごとに、同一のホストに対して、セッションIDの検証や生成を要求する構成とされてい

る、ためである。

【0006】また特開2000-222360号公報には、クライアント手段と、認証サーバ手段と、認可サーバ手段を備え、クライアント手段は、認証サーバと、秘密情報を共有し、認証サーバ手段は、秘密情報を不可逆演算 f を n 回行った照合情報を含む認証チケットを発行し、クライアント手段は認可サーバに、不可逆演算 f を $n-k$ 回行った提示情報を示し、認可サーバは、提示情報に不可逆演算 f を k 回行って照合情報と一致するかチェックする認証システム、方法が提案されている。このシステムも、認証サーバ手段と、認可サーバ手段に接続できない、WWWサーバ、端末では、適用できない。また、例えば特開平10-177552号公報には、クライアントと複数のサーバ間に認証応答管理部を有する代理サーバを設け、認証応答管理部が、クライアントを認証し、一旦認証したクライアントについて複数のサーバに対する認証情報の応答を代行する認証応答方法と装置が開示されている。

【0007】

【発明が解決しようとする課題】したがって本発明が解決しようとする課題は、認証を行うサーバを利用できないWWWサーバでも、認証の連携を可能とする方法及びシステムと装置並びにプログラムを提供することにある。

【0008】

【課題を解決するための手段】前記課題を解決するための手段を提供する本発明に係る方法は、端末からネットワークを介してアクセスされる一の情報提供サーバが、前記端末から入力され前記一の情報提供サーバに送信された利用者情報と、前記一の情報提供サーバでの時間情報とから、認証情報を生成し、生成した前記認証情報を、前記端末に送信するステップと、前記端末からネットワークを介してアクセスされる情報提供サーバであって、認証の連携処理を行う情報提供サーバでは、前記端末から送信された前記認証情報を受け取り、前記認証情報を復号して利用者情報及び時間情報を取り出し、認証判定を行うステップと、を含む。

【0009】本発明に係る方法は、端末が、利用者からの要求と、利用者認証を行うための利用者情報を、一の情報提供サーバに送信するステップと、前記一の情報提供サーバでは、前記利用者情報を、認証サーバに送信し、前記認証サーバでの認証が成功した場合に、前記一の情報提供サーバの認証情報生成部にて、認証情報を生成するステップと、前記一の情報提供サーバは、前記一の情報提供サーバの前記認証情報生成部で生成された前記認証情報を、要求結果と共に、前記端末に送信するステップと、前記端末が、前記一の情報提供サーバと連携し、認証の連携処理を行う他の情報提供サーバに要求を送信する場合、前記認証情報を、前記他の情報提供サーバを送信するステップと、前記他の情報提供サーバで

は、前記端末から送信された前記認証情報を受け取り、認証連携処理部で、前記認証情報を基に、認証の連携処理を行うステップと、前記他の情報提供サーバにおいて、前記認証の連携処理によって、認証情報の正しさが検証され、前記利用者が認証された場合には、前記利用者の要求を受け付け、要求結果と共に、新たに生成した認証情報を、前記端末に送信するステップと、を有する。

【0010】別のアспектにおいて、本発明に係るシステムは、端末からネットワークを介してアクセスされる一の情報提供サーバが、前記端末から入力され前記一の情報提供サーバに送信された利用者情報と、前記一の情報提供サーバでの時間情報とから、認証情報を生成し、生成した前記認証情報を、前記端末に送信する手段を備え、前記端末からネットワークを介してアクセスされる情報提供サーバであって、認証の連携処理を行う情報提供サーバが、前記端末から送信された前記認証情報を受け取り、前記認証情報を復号して利用者情報及び時間情報を取り出し、認証判定を行う手段を備えている。

【0011】さらに、別のアспектにおいて、本発明に係るプログラムは、端末からネットワークを介してアクセスされる一の情報提供サーバが、(a)前記端末から利用者からの要求と、利用者認証を行うための利用者情報を受信し、前記利用者情報を、前記認証サーバに送信する処理と、(b)前記認証サーバでの認証が成功した場合に、前記利用者情報と時間情報から認証情報を生成する認証情報生成処理と、(c)前記生成された認証情報を、要求結果と共に、前記端末に送信する処理と、を有し、端末からネットワークを介してアクセスされ前記一の情報提供サーバと認証の連携処理を行う情報提供サーバが、(d)前記端末から送信された前記認証情報から、利用者情報と時間情報を取り出し、認証の連携処理を行う認証連携処理と、(e)前記認証連携処理によって、認証情報の正しさが検証され、前記利用者が認証された場合は、前記利用者の要求を受け付け、要求結果と共に、新たに生成した認証情報を、前記端末に送信する処理とを含み、前記各処理を前記各情報提供サーバで実行させるためのプログラムよりなる。

【0012】

【発明の実施の形態】本発明の実施の形態について説明する。本発明は、その好ましい一実施の形態において、ブラウザ機能を有する端末(図1の1)から、IP(Internet Protocol)網等のネットワークを介してアクセスされる情報提供サーバ(WWW(World Wide Web)サーバ)(図1の2)が、端末(図1の1)から入力されWWWサーバ(2)に送信された利用者情報を受け取る手段(図1の21)と、利用者情報と、前記一のWWWサーバでの時間情報とから、認証情報を生成する手段(図1の23)と、生成した前記認証情報を、前記端末に送信する手段(図1の21)を備えている。また端末(図

1の1)からネットワークを介してアクセスされ、認証の連携処理を行うWWWサーバ(図1の3)は、端末(図1の1)から送信された認証情報を受け取る手段(図1の31)と、該認証情報を復号して利用者情報及び時間情報を取り出し、時間検査を行うことで認証判定を行う手段(図1の34)を備えている。

【0013】本発明は、その好ましい一実施の形態において、認証サーバ(図1の4)に接続される一のWWWサーバ(図1の2)は、端末(図1の1)が、利用者からの要求と、利用者認証を行うための利用者情報を、WWWサーバ(図1の2)に送信した場合、これを受信し、前記利用者情報を認証サーバ(図1の4)に送信する手段(図1の21、22)と、認証サーバ(図1の4)での認証が成功した場合に、前記利用者の前記利用者情報と時間情報から認証情報を生成する認証情報生成手段(図1の23)と、前記生成された認証情報を、要求結果と共に、前記端末に送信する手段(図1の21)と、を備えている。

【0014】端末(図1の1)は、認証の連携処理を行うWWWサーバ(図1の3)に要求を送信する場合、WWWサーバ(図1の2)より送信された前記認証情報を、認証の連携処理を行う前記WWWサーバ(図1の3)に送信する手段(図1の11)を備えている。

【0015】認証の連携処理を行うWWWサーバ(図1の3)は、前記認証情報から、利用者情報と時間情報を取り出し、認証の連携処理を行う認証連携処理手段(図1の34)と、前記認証の連携処理によって、認証情報の正しさが検証され、前記利用者が認証された場合は、前記利用者の要求を受け付け、要求結果と共に、新たに生成した認証情報を、前記端末に送信する手段(図1の31)とを備えている。

【0016】本発明は、その好ましい一実施の形態において、前記一のWWWサーバで生成される認証情報が、利用者情報と時間情報と、チェックデータとを含み、これらの情報が暗号化されている。

【0017】認証の連携処理を行うWWWサーバ(図1の3)において、認証連携処理手段(図1の34)は、認証情報を復号する手段(図4のB1)と、復号された認証情報のチェックデータを検査する手段(図4のB2)と、該チェックデータの検査結果が正しい場合、復号された認証情報から利用者情報と時間情報を取り出す手段(図4のB3)と、前記時間情報の検査を行う手段(図4のB4)と、を含み、前記時間情報の検査結果が正しい場合、認証成功とする。

【0018】本発明の別の実施の形態において、上記した認証情報生成手段(図5の23)を備えたWWWサーバ(図5の5)が、認証連携処理手段(図5の54)をさらに備えた構成としてもよい。WWWサーバ(図5の5)は、端末(図5の1)から送信された認証情報を受け取り、認証連携処理手段(図5の54)で認証連携を行

い、認証判定が成功した場合、認証情報生成手段（図5の54）に対して認証情報の生成を依頼し、認証情報生成手段（図5の23）は、認証連携処理手段（図5の54）が前記認証情報から取得した利用者情報を受け取り、利用者情報と時間情報から認証情報を生成する。

【0019】認証の連携処理を行うWWWサーバ（図5の6）が、認証情報生成手段（図5の63）をさらに備えた構成としてもよい。認証の連携処理を行う前記WWWサーバ（図5の6）が、前記認証連携処理手段（図5の34）で認証連携を行い、認証判定が成功した場合、認証の連携処理を行うWWWサーバ（図5の6）の前記認証情報生成手段（図5の63）に認証情報の生成を依頼し、前記認証情報生成手段（図5の63）が、前記認証連携処理手段（図5の34）が前記認証情報から取得した利用者情報を受け取り、利用者情報と時間情報とから認証情報を生成し、利用者の要求結果と認証情報を前記端末に送信する。

【0020】WWWサーバにおける認証情報生成手段、認証連携処理手段は、WWWサーバのノードコンピュータで実行されるプログラムによりその処理、機能が実現される。

【0021】複数のWWWサーバが、利用者を認証する場合に、認証処理サーバが共通的に利用できない環境である場合には、WWWサーバが認証処理サーバを利用することなしに、利用者の認証の連携をできるようにしている。

【0022】図1は、本発明の一実施の形態のシステム構成を示す図である。図1において、端末（1）は、WWWサーバ（2）等にインターネットプロトコル網等のネットワークを介して接続され、端末（1）から入力された認証用の利用者情報は、WWWサーバ（2）を介して認証サーバ（4）に提供される。

【0023】端末（1）の利用者要求送受信手段（11）は、利用者からの要求を、WWWサーバ（2）の利用者要求処理手段（21）に送信する。送信される要求には、初回時には利用者認証を行うための利用者ID、パスワードなどのような利用者情報が共に送信される。

【0024】WWWサーバ（2）の利用者要求処理手段（21）は、利用者情報を認証要求手段（22）に送信する。認証要求手段（22）は、認証サーバ（4）の認証処理手段（41）にその利用者情報を送信し、その利用者が利用可能かの結果を待つ。

【0025】認証サーバ（4）の認証処理手段（41）で認証が成功した場合、認証成功という結果がWWWサーバ（2）の認証要求手段（22）に返され、認証要求手段（22）は、認証情報生成手段（23）に、認証情報の生成を依頼する。

【0026】WWWサーバ（2）の利用者要求処理手段（21）は、認証情報生成手段（23）によって生成された認証情報を、その要求結果と共に、端末（1）の利

用者要求送受信手段（11）に送信する。この認証情報には、利用者情報や時間情報が含まれ、利用者が続く要求を送信する場合、利用者要求送受信手段（11）が自動的に共に送信するようになっている。

【0027】続いて利用者が、WWWサーバ（2）と連携する第2のWWWサーバ（3）の利用者要求処理手段（31）に要求を送信した場合、共に、認証情報が送信される。

【0028】その場合、その認証情報を基に、WWWサーバ（3）の認証連携処理手段（34）で認証連携処理が行われる。

【0029】認証連携処理によって、認証情報の正しさが検証され、利用者が認証された場合は、その利用者の要求を受け付けることになるが、WWWサーバ（3）の利用者要求処理手段（31）は、その要求結果を、端末（1）の利用者要求送受信手段（11）に送信する。

【0030】これにより、認証処理サーバを利用することなしに、利用者連携を行うことを可能にする。

【0031】

【実施例】上記した実施の形態についてさらに具体的かつ詳細に説明すべく本発明の実施例について説明する。図1は、本発明の一実施例のシステム構成の一例を示す図である。図1を参照すると、本発明の一実施例に係るシステムは、利用者が要求を送受信する端末1と、その利用者要求を処理するWWWサーバ2と、WWWサーバ2と連携してその利用者要求を処理する第2のWWWサーバ3と、利用者の認証情報を処理する認証サーバ4とを含む。なお、この実施例において、WWWサーバが提供する情報の内容、種類は問わないが、処理要求の実行にあたり、利用者の認証が必要とされるものとする。

【0032】端末1は、利用者の要求をWWWサーバに送信し、WWWサーバからの処理結果を受信する利用者要求送受信手段11を備える。利用者要求送受信手段11は、要求を送信する際には、WWWサーバ2の認証情報生成手段23が生成した認証情報がある場合には、該要求と共に自動的に送信する。要求が処理された場合には、WWWサーバ2の利用者要求処理手段21や、WWWサーバ3の利用者要求処理手段31から送信される要求結果を受信する。

【0033】WWWサーバ2は、利用者要求処理手段21と、認証要求手段22と、認証情報生成手段23とを備える。

【0034】WWWサーバ2において、利用者要求処理手段21は、利用者要求送受信手段11から送られてきた要求を処理する。初回要求時には、要求と共に送信されてきた利用者ID、パスワードのような利用者情報を認証要求手段22に渡し、認証結果を得る。認証サーバ2での認証が成功し、WWWサーバ2が要求結果を、端末1に送信する際には、認証情報生成手段23にて生成された認証情報を、要求結果と共に、端末1の利用者要

求送受信手段 11 に送信する。

【0035】WWWサーバ2において、認証要求手段22は、利用者要求手段21から渡された利用者情報を、認証サーバ4の認証処理手段41に送信し、認証サーバ4のから認証結果を受け取る。

【0036】認証サーバ4で認証が成功した場合には、WWWサーバ2の認証要求手段22は、認証情報生成手段23に、認証情報生成を要求する。認証要求手段22は、認証情報生成手段23で生成された認証情報を、利用者要求処理手段21に返す。

【0037】WWWサーバ2において、認証情報生成手段23は、認証要求手段22からの要求に従い、認証情報を生成し、その結果を返す。認証要求手段22からは利用者情報が渡され、認証情報には、該利用者情報や時間情報が含まれる。

【0038】第2のWWWサーバ3は、利用者要求処理手段31と、認証連携処理手段34を備える。

【0039】第2のWWWサーバ3において、利用者要求処理手段31は、利用者要求処理手段21と同様、利用者要求送受信手段11から送られてきた要求を処理する。要求と共に送信されてきた認証情報を認証連携処理手段34に渡し、その結果を得る。認証が成功した場合は、要求結果を利用者要求送受信手段11に送信する。

【0040】第2のWWWサーバ3において、認証連携処理手段34は、利用者要求処理手段31から渡された認証情報に対し、正しさの検証を行う。利用者情報や時間情報から、認証情報の正しさが確認され、その結果を利用者要求処理手段31に返す。

【0041】認証サーバ4は、認証処理手段41と、利用者管理手段42とを備える。認証処理手段41は、認証要求手段22から利用者情報を受け取る。受け取った利用者情報は、利用者管理手段42に渡され適合する情報が探される。もし、利用者管理手段42で適合する情報が見つかった場合には、認証処理手段41は、「認証成功」の通知を、WWWサーバ2の認証要求手段22に返す。一方、利用者管理手段42で適合する情報が見つからなかった場合には、認証処理手段41は、「認証失敗」の通知を認証要求手段22に返す。

【0042】利用者管理手段42は、認証処理手段41から渡された利用者情報に対し、保持する管理情報から適合する情報を探し出し、その結果を受け渡す。

【0043】図2は、本発明の一実施例の動作を説明するためのフローチャートである。図1及び図2を参照して、本発明の一実施例の全体の動作について詳細に説明する。

【0044】端末1の利用者要求送受信手段11から利用者の要求が、WWWサーバ2の利用者要求処理手段21に送信される(図2のステップA1およびA2)。この場合、利用者情報が送信されるので、利用者要求処理手段21は、利用者情報を取り出す(図2のステップA

3)。

【0045】処理の結果、利用者要求処理手段21が利用者情報の取り出しに失敗した場合、利用者情報が利用者要求送受信手段11から正しく送信されてきていないものと判断し、利用者要求処理手段21は、エラーを、利用者要求送受信手段11に送信する(図2のステップA4)。

【0046】利用者要求送受信手段11は、エラーを受信し、その結果は、利用者に対して、端末1の表示装置の画面上に示される(図2のステップA5)。図2のステップA3において、正しく取り出された利用者情報は、認証要求手段22に渡され、さらに、認証サーバ4の認証処理手段41に、認証判定処理が要求される(図2のステップA6)。

【0047】認証サーバ4の認証処理手段41は、利用者情報を受信する(図2のステップA7)。さらに認証処理手段41は、認証が成功するか調べるため、対象となる利用者情報を利用者管理手段42に渡し、管理されている情報と適合するか調査を行う(図2のステップA8)。この処理は、例えば、コンピュータで行われている、利用者IDとパスワードの検査からなる。処理の結果として、認証が失敗した場合は、その結果が認証要求手段22に渡され、さらには利用者要求処理手段21が、エラーを、端末1の利用者要求送受信手段11に送信する(図2のステップA9)。

【0048】利用者要求送受信手段11は、エラーを受信し、その結果は、利用者に対し端末1の画面上等に表示される(図2のステップA10)。

【0049】図2のステップA8にて、認証判定が成功した場合、認証要求手段22は、その結果に従い、認証情報生成手段23に認証情報の生成を依頼する。その際、認証要求手段22から利用者情報が渡され、認証情報生成手段23は、受け取った利用者情報や、時間情報から、認証情報を生成する(図2のステップA11)。

【0050】生成された認証情報は、認証要求手段22から利用者要求処理手段21に「認証成功」という結果と共に受け渡される。利用者要求処理手段21は、利用者の要求結果と認証情報を、利用者要求送受信手段11に送信し、その結果は、利用者に対して端末1の画面上に示される(図2のステップA12、およびA13)。

【0051】引き続き、利用者が連携する第2のWWWサーバ3にアクセスするため、利用者要求送受信手段11から、利用者要求処理手段31に要求が送信される(図2のステップA14)。

第2のWWWサーバ3の利用者要求処理手段31は該要求を受信し(図2のステップA15)、利用者要求送受信手段11から該要求と共に自動的に送信された認証情報を取り出す(図2のステップA16)。処理の結果、利用者要求処理手段31が認証情報の取り出しに失敗した場合、利用者要求処理手段31は、認証情報が利用者要求送受信手段11から正

しく送信されてきていないものと判断し、エラーを、端末1の利用者要求送受信手段11に送信する(図2のステップA17)。端末1の利用者要求送受信手段11は、エラーを受信し、その結果は、利用者に対し端末1の画面上に示される(図2のステップA18)。

【0052】図2のステップA16において、第2のWWWサーバ3の利用者要求処理手段31で正しく取り出された認証情報は、利用者要求処理手段31から、認証連携処理手段34に渡される(図2のステップA19)。

【0053】第2のWWWサーバ3の認証連携処理手段34は、渡された認証情報に含まれる利用者情報や時間情報から、認証情報の正しさの検証を行う(図2ステップA20)。検証が成功しなかった場合は認証失敗となり、利用者要求処理手段31は、エラーを端末1の利用者要求送受信手段11に送信する(図2のステップA21)。

【0054】利用者要求送受信手段11は、エラーを受信し、その結果は利用者に対し端末1上に示される(図2のステップA22)。図2のステップA20において、認証判定が成功した場合、認証連携処理手段34は、利用者要求処理手段31に認証成功という結果を返す。利用者要求処理手段31は、利用者の要求結果を、端末1の利用者要求送受信手段11に送信し、その結果は利用者に対し端末1上に示される(図2のステップA23、およびA24)。

【0055】次に、図2のステップA11において生成される認証情報について説明する。図3は、生成される認証情報の一例を説明するための図である。図3に示すように、認証情報は、利用者情報や時間情報から成る。利用者情報は、図2のステップA1において送信される情報に含まれているものである。時間情報は、図1のWWWサーバ2やWWWサーバ3がシステムとして保持する現在時刻(システムクロックの示す現在の時刻情報；例えば年月日、時刻(時、分、秒)のタイムスタンプ)である。認証情報には、利用者情報や時間情報が組み合わされた情報から生成されるチェックデータが付加され、さらに、暗号化処理が施される。

【0056】図2のステップA20の認証連携判定処理について説明する。図4は、認証連携判定処理を説明するためのフローチャートである。

【0057】図4を参照すると、認証連携判定処理は、図3に示す暗号化された認証情報に対して、図4のステップB1にて、復号化が行われる。

【0058】復号化が行われた認証情報に対して、チェックデータの検証が行われる(図4のステップB2)。

【0059】図4のステップB2の結果として、チェックデータが異常の場合は、認証連携は失敗となる(図4のステップB5)。

【0060】チェックデータが正常の場合、利用者情報

と時間情報が取り出され(図4のステップB3)、時間情報が、図1の認証連携処理手段34に定められている時間内であるか否かの検証が行われる(図4のステップB4)。

【0061】この検証が失敗した場合には、認証連携は失敗と判断され(図4のステップB5)、検証が成功した場合には、認証連携成功と判断される(図4のステップB6)。

【0062】上記実施例で説明したWWWサーバ2の利用者要求処理手段21、認証要求手段22、及び認証情報生成手段23、WWWサーバ3の利用者要求処理手段31、認証連携処理手段34の各手段は、WWWサーバ2、3のコンピュータで実行されるプログラムによりその処理、機能が実現される。

【0063】次に、本発明の他の実施例について図面を参照して詳細に説明する。図5は、本発明の第2の実施例の構成を示す図である。図5を参照すると、本実施例は、WWWサーバ5が、図1に示した前記実施例のWWWサーバ2の構成に加え、認証連携処理手段54を備えている。またWWWサーバ6は、図1に示した前記実施例の第2のWWWサーバ3の構成に加え、認証要求手段62と認証情報生成手段63と、を備えている。すなわち、各WWWサーバは、利用者要求処理手段と、認証要求手段と、認証情報生成手段と、認証連携処理手段を備えている。

【0064】WWWサーバ5の認証連携手段54は、前記実施例における認証連携手段34と同様に、利用者要求手段21から渡された認証情報に対して、正しさの検証を行い、さらに、利用者情報や時間情報から、認証情報の正しさが確認され、認証が成功した場合には、認証情報生成手段23に対して新しい認証情報を要求し、生成されたその認証情報を、利用者要求処理手段21に返す。

【0065】WWWサーバ6の認証要求手段62は、利用者要求手段31から渡された利用者情報を、認証処理手段41に送信し、認証結果を受け取る。認証が成功した場合には、認証情報生成手段63に対して認証情報生成を要求し、生成されたその認証情報を利用者要求処理手段31に返す。

【0066】WWWサーバ6の認証情報生成手段63は、認証要求手段62からの要求に従い、認証情報を生成し、その結果を返す。

【0067】WWWサーバ6の認証要求手段62からは、利用者情報が渡され、認証情報にはその利用者情報や時間情報が含まれる。

【0068】図6は、本発明の第2の実施例の動作を説明するためのフローチャートである。図6のステップA1-A22で示される、本発明の第2の実施例における利用者要求送受信手段11、利用者要求処理手段21、認証要求手段22、認証情報生成手段23、認証処理手

段41および利用者管理手段42の動作は、図1に示された実施例の各手段11、21、22、23、41および42の動作（図2のステップA1-A22）と同一であるため、その説明は、省略する。

【0069】前記実施例では、認証連携処理手段34は、単に、認証情報の正しさのみを確認し、その結果を利用者要求処理手段31に返していた。

【0070】この実施例では、図6のステップA20にて、認証判定が成功した場合、WWWサーバ6の認証連携処理手段34は、認証情報生成手段63に、認証情報の生成を依頼する。

【0071】WWWサーバ6の認証情報生成手段63には、認証連携処理手段34によって認証情報から得られた利用者情報が渡され、その利用者情報や時間情報から認証情報が生成される（図6のステップC1）。生成された認証情報は、認証連携処理手段34から利用者要求処理手段31に認証成功という結果と共に受け渡される。

【0072】WWWサーバ6の利用者要求処理手段31は、利用者の要求結果と認証情報を、利用者要求送受信手段11に送信し、その結果は利用者に対し端末1上に示される（図6のステップA23、およびA24）。

【0073】このようにWWWサーバ6の認証連携処理手段63によって生成された認証情報が、端末1の利用者要求送受信手段11に渡されることで、さらなる認証連携処理を行うことができる。

【0074】次に、図5と図7を参照して、さらなる認証連携処理の動作について説明する。図5において、利用者が端末1からWWWサーバ5にアクセスするため、その要求が、利用者要求送受信手段11から、WWWサーバ5の利用者要求処理手段21に送信される（図7のステップD1）。

【0075】WWWサーバ5の利用者要求処理手段21はその要求を受信し（図7のステップD2）、利用者情報を取り出す（図7のステップD3）。処理の結果、利用者要求処理手段21が利用者情報の取り出しに成功した場合、利用者情報を用いた認証連携処理に移行する（図7のステップD4）。利用者情報を用いた認証連携処理は、図2のステップA6以降の処理と同一であるため、説明は省略する。

【0076】図7のステップD3にて、利用者要求処理手段21が利用者情報の取り出しに失敗した場合、利用者要求送受信手段11から要求と共に自動的に送信された認証情報を取り出す（図7のステップD5）。

【0077】処理の結果、利用者要求処理手段21が認証情報の取り出しに失敗した場合、認証情報が利用者要求送受信手段11から正しく送信されてきてないと判断し、利用者要求処理手段21はエラーを利用者要求送受信手段11に送信する（図7のステップD6）。

【0078】端末1の利用者要求送受信手段11はエラ

ーを受信し、その結果は利用者に対し端末1上に示される（図7のステップD7）。

【0079】図7のステップD5において、正しく取り出された認証情報は、利用者要求処理手段21から認証連携処理手段54に渡される（図2のステップD8）。認証連携処理手段54は、渡された認証情報に含まれる利用者情報や時間情報から、認証情報の正しさの検証を行う（図7ステップD9）。

【0080】検証が成功しなかった場合は、認証失敗となり、利用者要求処理手段21がエラーを利用者要求送受信手段11に送信する（図7のステップD10）。

【0081】利用者要求送受信手段11は、エラーを受信し、その結果は、利用者に対し端末1上に示される（図7のステップD11）。

【0082】図7のステップD9にて認証判定が成功した場合、認証連携処理手段54は、認証情報生成手段23に認証情報の生成を依頼する。

【0083】認証情報生成手段23には、認証連携処理手段54によって認証情報から得られた利用者情報が渡され、その利用者情報や時間情報から、認証情報が生成される（図7のステップD12）。

【0084】生成された認証情報は、認証連携処理手段54から利用者要求処理手段21に認証成功という結果と共に受け渡される。

【0085】利用者要求処理手段21は、利用者の要求結果と認証情報を、利用者要求送受信手段11に送信し、その結果は利用者に対し端末1上に示される（図2のステップD13、およびD14）。

【0086】図7のステップD13に引き続き、図5に示すシステム構成において、利用者がさらにWWWサーバ6にアクセスをする場合、これは、図2のステップA14以降と同様の処理で認証連携を処理することができる。図5に示すシステム構成において、端末1から利用者がさらにWWWサーバ5にアクセスをする場合、これは、図7のステップD1以降と同様の処理で認証連携を処理することができる。

【0087】また、図5に示すシステム構成において、利用者がWWWサーバ6に最初アクセスをする場合でも、図6の各処理においてWWWサーバ5とWWWサーバ6を置き換えれば、同一の動作で処理を行うことができる。

【0088】この第2の実施例は、すべてのWWWサーバが、認証連携処理手段と認証情報生成手段を持つため、利用者からの要求が複数回続く場合でも、すべてのWWWサーバで認証連携を処理できるという新たな効果を有する。また、さらに認証処理サーバが共通的に利用できる同一構成のWWWサーバから成る分散環境において、利用者からWWWサーバへの最初のアクセスのみに、認証サーバを利用する利用者認証処理が行われ、続くアクセスでは認証連携処理が行われるため、認証処理

サーバへのアクセス回数が少なくなり、利用者の要求へのレスポンス送信時間が短縮できるという新たな効果を有する。

【0089】

【発明の効果】以上説明したように、本発明によれば、情報提供サーバ（WWWサーバ）間で利用者認証連携をする場合に、すべての情報提供サーバが認証処理サーバを利用できない環境においても、利用者認証ができることである、という効果を奏する。

【0090】その理由は、本発明においては、認証サーバで利用者情報により認証された後に生成される認証情報が、認証処理サーバを利用できない情報提供サーバの認証連携処理手段によって、認証サーバにアクセスすることなしに、その正当性が確認される、構成としたためである。

【図面の簡単な説明】

【図1】本発明の一実施例のシステム構成を示す図である。

【図2】本発明の一実施例の動作を説明するための流れ図（フローチャート）である。

【図3】本発明の一実施例における認証情報の作成を説

明するための図である。

【図4】本発明の一実施例における認証連携処理の動作を説明するための流れ図（フローチャート）である。

【図5】本発明の他の実施例のシステム構成を示す図である。

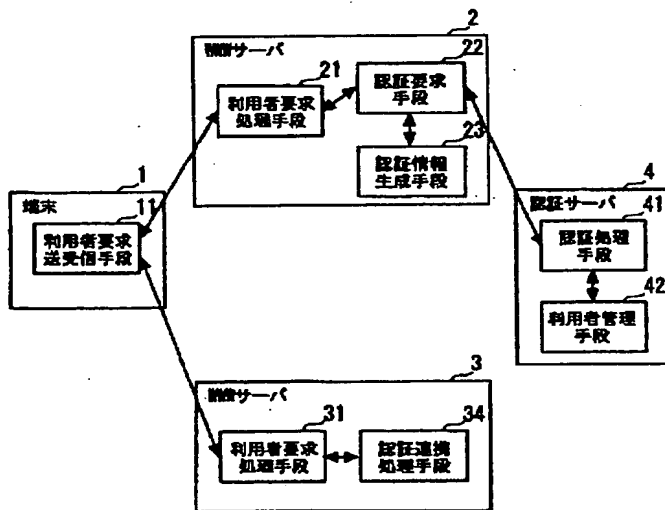
【図6】本発明の他の実施例の動作を説明するための流れ図（フローチャート）である。

【図7】本発明の他の実施例の認証連携処理の動作を説明するための流れ図（フローチャート）である。

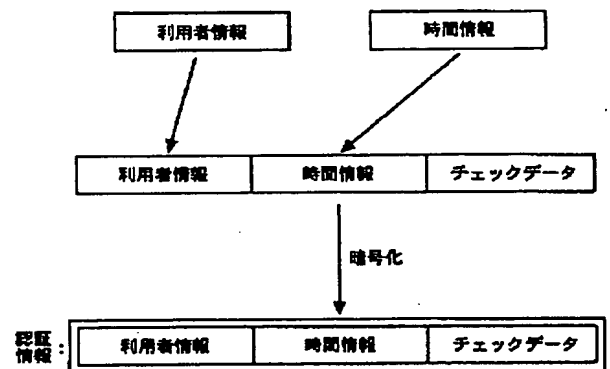
【符号の説明】

- 1 端末
- 2、3、5、6 WWWサーバ
- 4 認証サーバ
- 11 利用者要求送受信手段
- 21 利用者要求処理手段
- 22 認証要求手段
- 23、63 認証情報生成手段
- 31 利用者要求処理手段
- 34、54 認証連携処理手段
- 41 認証処理手段
- 42 利用者情報管理手段

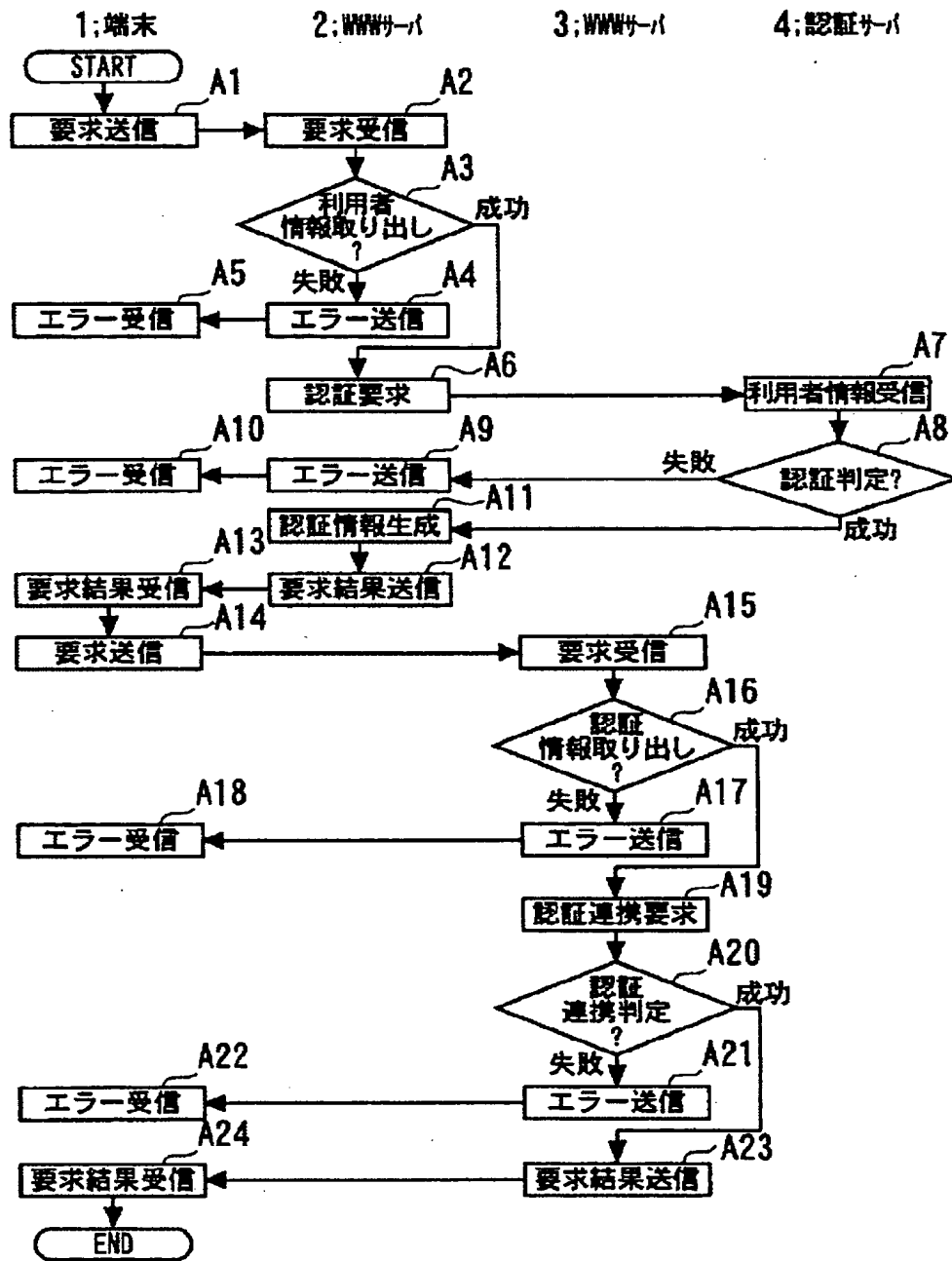
【図1】



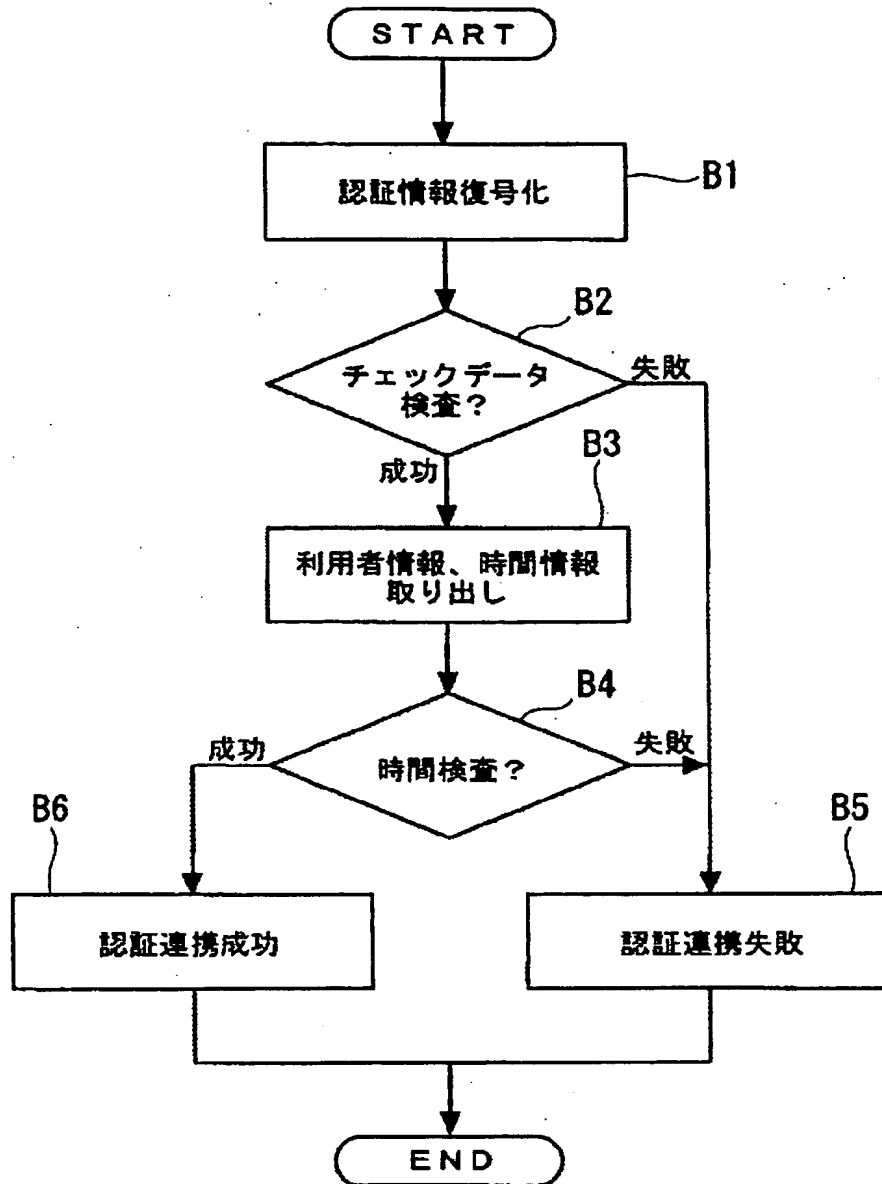
【図3】



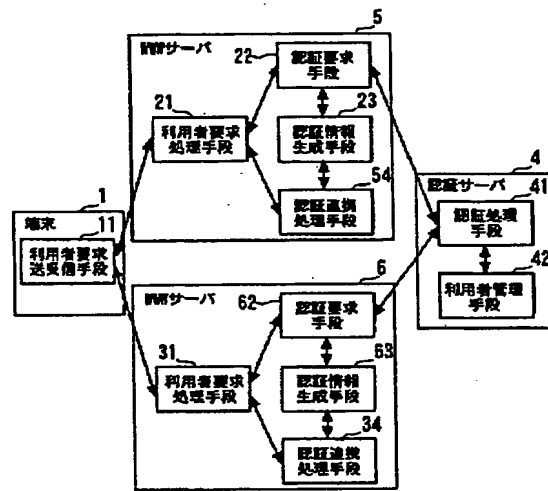
【図2】



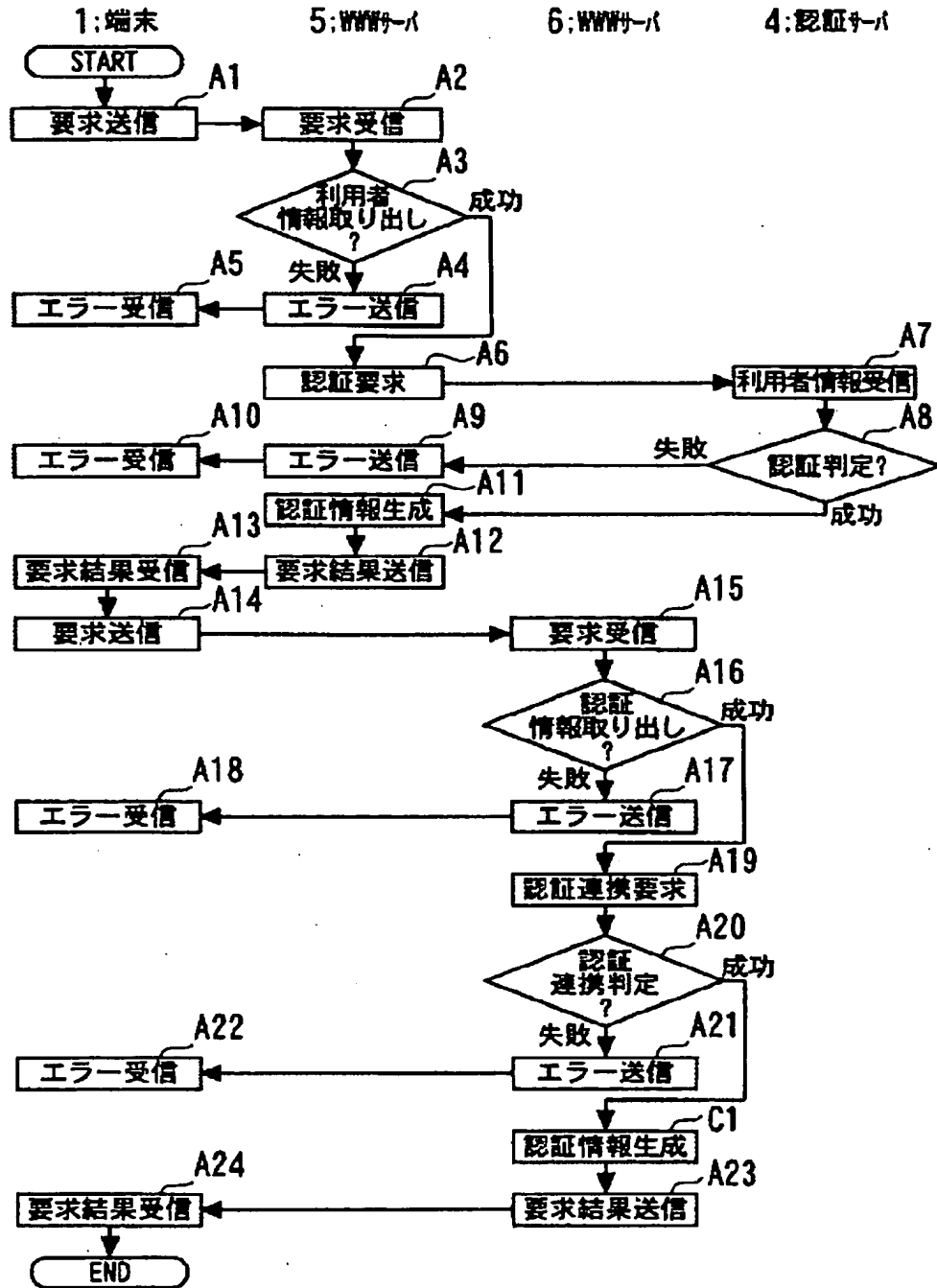
【図4】



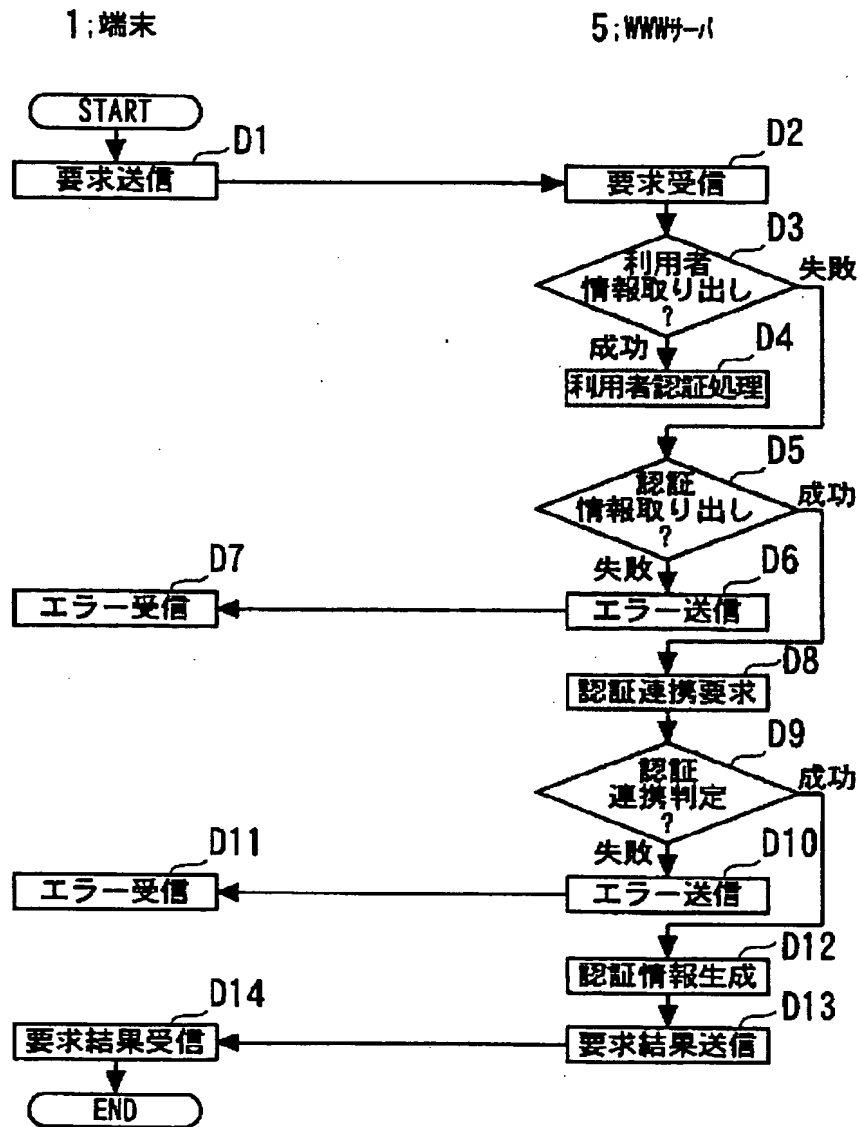
【図5】



【図6】



【図7】



**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☒ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

This Page Blank (uspto)